

OUCH!

Tässä numerossa...

- Tabletilaitteesi suojaaminen
- Turvallisena pysyminen

Uuden tabletilaitteesi suojaaminen

Yleiskatsaus

Onnittelut uudesta taulutietokoneestasi! Tabletit ovat tehokkaita ja käteviä laitteita kommunikointiin, verkko-ostoksiin, elokuvien katselemiseen, pelien pelaamiseen ja moniin muihin tarkoituksiin. Koska laitteestasi tulee todennäköisesti tärkeä osa päivittäistä elämääsi ja ehkä jopa korvaa tietokoneesi, tässä uutiskirjeessä on kuvattu keinoja, joilla saat turvattua tablettisi ja siinä olevat tiedot.

Vierastoimittaja

Lori Rosenbergilla on laaja kokemus tietoturvakoulutusmateriaalien tuottamisesta ja lisäksi hän järjestää aiheesta koulutuksia työntekijöille ja asiakkaille. Lori yrittää jatkuvasti löytää uusia ja mukaansatempaavia tapoja jakaa tietoturvatietoisuutta. Löydät hänet Twitteristä [@InfoSecLori](#).

Tabletilaitteesi suojaaminen

Saattaa olla yllättävää, että suurin taulutietokonettasi uhkaava riski ei ole hakkerit, vaan sinä itse. Todennäköisesti laite hukkuu, unohtuu tai rikkoontuu ennen kuin kukaan hakkeroi sitä. Ensimmäinen asia mitä tabletille kannattaa siksi tehdä on asettaa näyttö lukittumaan automaattisesti. Tämä tarkoittaa sitä, että laite pitää joka kerta avata sormenjäljellä, pääsykoodilla, eleellä tai muulla tunnistautumistavalla. Tällä varmistut siitä, että vaikka laitteesi katoaa, kukaan ei pääse käsiksi tietoihisi. Kun olet asettanut laitteen automaattisen lukitsemisen, tässä on muita oleellisia vinkkejä laitteesi suojaamiseen:

1. Asenna laitevalmistajan etävalvontasovellukset. Tämän avulla voit paikallistaa laitteesi jos se katoaa ja myös tyhjentää laitteen etänä jos se on varastettu.
2. Päivitä laitteesi käyttämä käyttöjärjestelmä ja salli automaattiset päivitykset. Hyökkääjät pyrkivät käyttämään hyväkseen laitteiden haavoittuvuuksia, jotka usein korjataan päivitysten yhteydessä. Varmista siis, että käytät aina uusinta käyttöjärjestelmää ja sovellusversioita.
3. Tarkista laitteen käyttöönoton yhteydessä laitteen asetukset, erityisesti yksityisyyteen liittyvät. Suurin haaste liittyy yleensä laitteen paikantamiskykyihin, jonka avulla sovellukset ja muut käyttäjät pystyvät paikallistamaan sijaintisi. Poista paikantaminen laitteelta ja salli se tämän jälkeen erikseen vain niille sovelluksille, joita pidät turvallisena ja jotka mielestäsi tarvitsevat tätä ominaisuutta. Huomaa, että jotkut sovellukset, kuten kartat tarvitsevat paikantamisominaisuutta

Uuden tabletilaitteesi suojaaminen

toimiakseen, mutta suurin osa sovelluksista ei tarvitse ajantasaista tietoa sijainnistasi.

4. Monet laitteet ja sovellukset käyttävät pilvipalveluita tietojesi tallentamiseen. Varmista, että tiedät missä tietosi on ja miten ne on turvattu. Et varmaankaan halua, että yksityiset kuvasi päätyvät kaikkien nähtäväksi sisäänrakennettuine sijaintitietoineen. Varmista, että jakaminen on oletuksena poistettu käytöstä ja salli se vain, kun haluat jakaa jotain tiettyä tietoa muille.
5. Pilvipalveluihin liittyen, tabletit myös synkronisoivat usein sovellustesi tai laitteesi tietoja muiden laitteiden tai sovellusten kanssa. Tämä on erittäin hyödyllinen ominaisuus joissain tapauksissa, mutta tarkista mitä tietoja laitteesi synkronisoi, jotta vain haluamasi tiedot jaetaan.



Parhaat keinot tabletilaitteen turvalliseen käyttöön ovat näytön lukitseminen, yksityisyysasetusten läpikäynti ja laitteen säännöllinen päivittäminen .

Turvallisena pysyminen

Kun olet suojannut taulutietokoneesi, varmista että se pysyy turvallisena myös jatkossa. Seuraavana on joitakin keinoja, joilla varmistat laitteen jatkuvan turvallisen käytön.

- Älä "jailbreikkaa" tai "roottaa" laitettasi. Tällaiset toimet ohittavat tai heikentävät laitteen turvallisuuskontrolleja ja altistavat laitteesi erinäisille hyökkäyksille.
- Lataa vain tarvitsemiasi sovelluksia ja ainoastaan luotettavista lähteistä. Käytä Applen laitteille vain Applen omaa sovelluskauppaa, kaikki siellä tarjolla olevat sovellukset ovat Applen tarkastamia ja hyväksymiä. Google-käyttöjärjestelmällä toimiville laitteille suosittelemme lataamaan sovelluksia vain Google Playstä ja Amazonin laitteille vain Amazonin-sovelluskaupasta. Sovelluksia voi ladata myös muista lähteistä, mutta näitä ei ole tarkistettu sovellustoimittajan toimesta ja ne saattavat sisältää haittaohjelmia. Kun et enää tarvitse tiettyä sovellusta, se kannattaa poistaa.
- Kun asennat uuden sovelluksen, varmista myös sovelluksen asetukset, mukaan lukien yksityisyysasetukset aivan kuten teit laitteen käyttöönoton yhteydessä. Varmista, että sovellus pääsee käsiksi vain niihin tietoihin mitä se oikeasti tarvitsee, esim. tarvitseeko sovellus oikeasti pääsyn kontakteihisi ja valokuviin. Jos et ole varma tarvitseeko

Uuden tabletilaitteesi suojaaminen

sovellus joitain tietoja, yritä etsiä toinen vastaava sovellus joka sopii paremmin käyttötarkoituksisi tai varmista mihin sovellus näitä tietoja käyttää. Huomaa myös, että päivittyessään sovellukset saattavat muuttaa asetuksia.

Tabletilaitteesi on tehokas työkalu, josta käytöstä haluamme sinun nauttivan. Muistamalla nämä muutamat ohjeet joilla pidät tablettisi ja tietosi turvassa.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-utiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa <http://www.securingthehuman.org>.

Elisa Appelsiini on korkean osaamisen IT-palvelutalo. Noin 400 IT-alan ammattilaisen voimin tuotamme monipuolisia ja tietoturvallisia tietotekniikkaan liittyviä pilvi-, työn tuottavuus-, konsultointi- ja ulkoistuspalveluja. Kehitämme myös asiakkaidemme liiketoimintaa tukevia sovelluksia ja tuotteita. Toimintamme perustuu syvään teknologiaosaamiseen ja aidosti asiakaslähtöiseen toimintaan.

Elisa Appelsiini is a comprehensive IT service provider owned by the leading provider of communications services in Finland, Elisa. Elisa Appelsiini helps its customers to enhance their business and increase competitiveness by offering high-end IT services in consulting, cloud, integration, software development and outsourcing.

Lähteet

- Mobiilisovellusten turvallinen käyttö: <https://www.securingthehuman.org/ouch/2015#january2015>
- Salasanalausekkeet: <https://www.securingthehuman.org/ouch/2015#april2015>
- Pilvipalveluiden turvallinen käyttö: <https://www.securingthehuman.org/ouch/2014#september2014>
- Mobiililaitteiden hävittäminen: <https://www.securingthehuman.org/ouch/2014#june2014>
- SANS Päivän tietoturvavinkki: https://www.sans.org/tip_of_the_day.php

Lisenssi

OUCH! julkaisijana toimii "SANS Securing The Human"-organisaatio ja jakelu tapahtuu [Creative Commons BY-NC-ND 3.0 lisenssillä](https://creativecommons.org/licenses/by-nc-nd/3.0/). Voit vapaasti jakaa tätä uutiskirjettä ja käyttää sitä osana tietoturvatietoisuusohjelmaasi kunhan et muokkaa uutiskirjettä. Käännös- ja lisätietoja varten, ota yhteys www.securingthehuman.org/ouch. Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy



securingthehuman.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.org/gplus